TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission	17

Application No.	09/896,380
Filing Date	June 29, 2001
First Named Inventor	Gary L. Graunke
Art Unit	2136
Examiner Name	Shiferaw, E.
Attorney Docket Number	42390P11153

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☒ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
  - ☐ PTO/SB/08
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Basic Filing Fee
  - ☐ Declaration/POA
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s)
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below):*

Return postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Gordon R. Lindeen III, Reg. No. 33,192 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	December 7, 2006

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	**Debbie Casias**		
Signature	Debbie Casias	Date	**December 7, 2006**

FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT	($)	500.00

Complete if Known	
Application Number	09/896,380
Filing Date	June 29, 2001
First Named Inventor	Gary L. Graunke
Examiner Name	Shiferaw, E.
Art Unit	2136
Attorney Docket No.	42390P11153

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 02-2666 Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20. ☒ Credit any overpayments

FEE CALCULATION

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	500.00
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify) _____

SUBTOTAL (2) ($) 500.00

SUBMITTED BY Complete (if applicable)

Name (Print/Type)	Gordon R. Lindeen III	Registration No. (Attorney/Agent)	33,192	Telephone	(303) 740-1980
Signature				Date	12/07/06

Based on PTO/SB/17 (12-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 12/15/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Our Docket No.: 42390P11153

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Gary L. Graunke	)	Examiner: Shiferaw, Eleni A.
	)	
Application No.: 09/896,380	)	Art Group: 2136
	)	
Filed: June 29, 2001	)	
	)	
For: Method and Apparatus for Simultaneous Encryption and Decryption of Publicly Distributed Media	)	

Mail Stop: Appeal Brief - Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

Applicant (hereinafter "Appellant") hereby submits this Appeal Brief (hereinafter "Brief") in support of its appeal from a final decision by the Examiner, mailed July 7, 2006, in the above-referenced Application. Appellant respectfully requests consideration of this appeal by the Board of Patent Appeals and Interferences (hereinafter "Board") for allowance of the above-captioned patent application.

An oral hearing is not desired.

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation of 2200 Mission College Boulevard, Santa Clara, California 95052.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

III. STATUS OF THE CLAIMS

Claims 1-21 are currently pending in the above-referenced application. No claims have been allowed. All pending claims were rejected in the Final Office Action mailed July 7, 2006, and are the subject of this appeal.

All pending claims stand rejected under 35 U.S.C. § 103.

IV. STATUS OF AMENDMENTS

In response to the Final Office Action mailed on July 7, 2006, rejecting claims 1-21, Appellant timely filed a Notice of Appeal on October 9, 2006.

A copy of all claims on appeal is attached hereto as Appendix A.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

The following paragraphs of the originally filed specification are believed to be instructive in considering the present application.

"[0002] Many different approaches have been taken to prevent unauthorized reproduction and distribution of content such as movies and videos, software and television programming. Most of these approaches have focused on one of two portions of vulnerability of the content. The first portion is the distribution media to the end customer....

"[0004] The second portion of the vulnerability is the use of the content after receipt by the end customer....

"[0005] In any combination of these systems, the content is decrypted at some point in the distribution chain and at that point becomes vulnerable to unauthorized reproduction and distribution. If the set-top box, which receives the media, is a flexible software driven box such as a personal computer, then the software which performs the decryption as well as the content of the media, may be accessible to users that attempt to produce unauthorized copies. This leaves the content vulnerable, notwithstanding the various efforts that have been applied to encrypt and protect it."

Claim 1 refers to a method with the following elements:

receiving first (K1) and second (K2) encryption keys from a key server 17 (*See page 8, lines 16-20, page 9, lines 19-23*);

receiving encrypted video 13 from a broadcast video source 11 (*See page 10, lines 1-5*);

generating a first cipher stream based on the a first key for decrypting the encrypted video (*See page 11, lines 20-23*);

generating a second cipher stream based on the a second key to re-encrypt the decrypted video (*See page 11, lines 20-23*);

simultaneously decrypting and re-encrypting the encrypted video using a combination 31 (SK1^SK2) of the first and the second cipher streams (*See page 10, lines 2-7, lines 12-16, page 11, line 22 to page 12, line 3, page 14, lines 1-3*);

conveying the re-encrypted video to a display device 27 to be decrypted by the display device using the second key (*See page 10, lines 6-7*).

Claim 12 is similar and present the invention based on the format of *In re Beauregard.* A machine is shown in as element 15 and 25 and 400 in Figure 4 and a machine-readable medium may include mass storage device 407. These are described on page 16, line 1 to page 18, line 15.

Claim 17 is similar to Claim 1 and finds additional support in the description of Figure 4 on page 16, line 1 to page 18, line 15. The content interface is exemplified by interface 426, the key interface is exemplified by communication device 425. The computing device is exemplified by processor 402, and the sink interface is exemplified by interfaces 427 and 429. Appropriate hardware is also described in the locations specified for Claim 1.

Claim 3 refers to the cipher stream combination comprising a result of exclusive OR-ing the first and second cipher streams (*See page 11, line 22 to page 12, line 3*).

Claim 10 refers to the encrypted video is publicly available and encrypted with a public key and the first key is a locally available private key (*page 14, lines 5-13*)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-26 stand rejected under 35 U.S.C. §103 (a) as being unpatentable over Kamiya et al., U.S. Publication No. US 2002/0106086 A1 ("Kamiya"), in view of Menezes et al., Menezes, Handbook of Applied Cryptography, ("Menezes").

The remaining rejections rely on this rejection. Only this first rejection is to be reviewed.

VII. ARGUMENT

A. Summary

Applicant's position may be summarized as follows. The present invention is unique in:

a) combining a decryption cipher stream and an encryption cipher stream;

b) using this combination to simultaneously decrypt and re-encrypt data; and

c) applying this approach to video delivery.

Applicant respectfully submits that this is simply not shown in either reference.

B. Neither Kamiya nor Menezes show simultaneous encryption and decryption

As agreed upon by both sides, Kamiya shows a decryption server 33 in Figure 1 that performs decryption and scrambling. The box is expanded in Figure 4 and, as shown there, it has a decryption unit 35A, a content decoding unit 35C, and a scramble unit 35D. The decryption unit uses a restored key combined at 35B from two keys A1 from 18, and A2 from 19 both based on A from 16 at the broadcaster.

The decrypted digital data is passed in the clear to the content decoding unit 35C for decoding and then to the scramble unit 35D. The scramble unit scrambles the digital data using a scramble key obtained from the scramble control unit 36. The scrambled digital data is then passed to the output device descramble unit 34A to be descrambled using a descramble key from the scramble control unit. The scramble key and the descramble key may be the same.

The decoder 35C is in between the decryption unit 35A and the scramble unit 35D. Its function is described only in paragraphs 79, 80 and 104. It is an MPEG or wavelet transform decoder. This has nothing to do with decryption but instead it is about converting digital bit streams into video or audio. MPEG video is encoded primarily for compression reasons. For example, some data is converted into video by applying codewords to a look-up table, the data for some video frames is expressed as the

difference from nearby frames, so the total information for such a frame can only be determined by decoding the nearby frames and applying the difference information. The decoded video is not described but is applied directly to the display (after scrambling and descrambling) so it most likely is a conventional full video signal that provides a complete (analog or digital) bitmap for each frame. The decoding process is standardized and well-documented and has nothing to do with security or encryption. It can only be performed once the data has been decrypted.

The intermediate decoding step requires that the decryption and the scrambling not be combined or performed simultaneously.

Claim 1, however, recites "simultaneously decrypting and re-encrypting the encrypted content using a combination of the first and the second cipher streams." There is no suggestion in Kamiya of simultaneously decrypting and re-encrypting nor of using a combination of a first and a second cipher stream. Kamiya uses a combination key for decryption only. Another key, the scramble key is used to scramble. Importantly in Kamiya, the decryption unit and the scramble unit perform separate unrelated processes using two different keys. The decryption and the scramble process cannot be simultaneous because there is a content decoding process in between.

Menezes §§7.26 to 7.42 describes encryption and attacks with very little mention of decryption. There is no mention of decrypting with one key and encrypting with another. There is no mention of combining an encryption key with a decryption key. There is no mention of simultaneously encrypting and decrypting. In addition, there is not even any mention of combining encryption keys or simultaneously encrypting with two keys. The cascade cipher (§7.29) uses independent keys to encrypt in stages. The multiple encryption (§7.30) also uses different keys applied in different stages but the same key can be used more than once. This is further brought out in §7.40(iii) in which multiple modes may be "pipelined." Pipelining allows multiple operations to be performed quickly in series. It does not suggest simultaneous but sequential.

The Examiner refers to "CBC of multiple encryption method." Sections 7.40 and 7.41 refer to CBC. Section 7.40 refers to a composite operation of triple encryption and to sequential applications of operations. A composite operation is an operation made up of distinct parts. In other words, as in the other examples, Menezes takes different keys

and applies them sequentially (one at a time) to the data. Applicant is unable to find any mention here of decrypting and re-encrypting but only encrypting and breaking the encryption.

Consider again the limitations of Claim 1. First consider, "simultaneously decrypting and re-encrypting the encrypted video." Simultaneous is occurring at the same time. In Kamiya, first the decryption happens, then the decoding happens, then the scrambling happens. In Menezes, there is no suggestion of decrypting and then re-encrypting.

Second consider "decrypting and re-encrypting using a combination of the first and the second cipher streams." A combination is the result of combining two things, here the first and second cipher streams. In Kamiya, the restored decryption key must be kept separate from the scrambling key so that the two operations may be performed separately. In Menezes, decryption and encryption keys are not combined. Encryption keys are not even combined except to make a third additional key in multiple encryption.

Since neither reference teaches or suggests these two limitations, Claim 1 is believed to be allowable.

C. Neither Kamiya nor Menezes show exclusive OR-ing a decryption stream with an encryption stream

Claim 3 recites that "the cipher stream combination comprises a result of exclusive OR-ing the first and second cipher streams." Applicant is unable to find any suggestion in either reference of exclusive OR-ing a decryption cipher stream with an encryption cipher stream.

D. Neither Kamiya nor Menezes show a public encryption key and a private re-encryption key

Claim 10 recites that the encryption key is a public key and the re-encryption key is a local private key. The Examiner refers to Kamiya paragraph 21. This paragraph discusses public keys but does not mention local private keys.

VIII. CONCLUSION

Appellant respectfully submits that all appealed claims in this application are patentable and were improperly rejected by the Examiner during prosecution before the United States Patent and Trademark Office. Appellant respectfully requests that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

This Brief is submitted with a check for $500.00 to cover the appeal fee for one other than a small entity as specified in 37 C.F.R. § 1.17(c). Please charge any shortages and credit any overpayments to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: December 7, 2006

Gordon R. Lindeen III
Reg. No. 33,192

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA. 90025-1030
(303) 740-1980

IX. APPENDIX OF CLAIMS (37 C.F.R. § 41.37(c)(1)(viii))

1. A method comprising:

receiving first and second encryption keys from a key server;

receiving encrypted video from a broadcast video source

generating a first cipher stream based on the ~~a~~ first key for decrypting the encrypted video;

generating a second cipher stream based on the ~~a~~ second key to re-encrypt the decrypted video;

simultaneously decrypting and re-encrypting the encrypted video using a combination of the first and the second cipher streams;

conveying the re-encrypted video to a display device to be decrypted by the display device using the second key.

2. The method of Claim 1, wherein simultaneously decrypting and re-encrypting the encrypted video comprises exclusive OR-ing the encrypted video with the cipher stream combination.

3. The method of Claim 1, wherein the cipher stream combination comprises a result of exclusive OR-ing the first and second cipher streams.

4. The method of Claim 3, wherein the first key and the second key have symmetric agreement.

5. The method of Claim 1, wherein receiving the first and second encryption keys comprises receiving one or more of the first key and the second key over a secure authenticated channel.

6. The method of Claim 5, wherein receiving a key over a secure authenticated channel comprises receiving the key from a sales server.

7. The method of Claim 5, wherein the secure authenticated channel comprises an Internet connection.

8. The method of Claim 5, wherein the secure authenticated channel comprises a telephone line.

9. The method of Claim 1, further comprising conveying the second key to the display device to enable the display device to decrypt the re-encrypted video.

10. The method of Claim 1, wherein the encrypted video is publicly available and encrypted with a public key and wherein the first key is a locally available private key.

11. The method of Claim 1, wherein the encrypted video is a broadcasted entertainment program.

12. A machine-readable medium having stored thereon data representing sequences of instructions which, when executed by a machine, cause the machine to perform operations comprising:

receiving first and second keys from a key server;

receiving encrypted video from a broadcast video source

generating a first cipher stream based on the ~~a~~ first key for decrypting the encrypted video;

generating a second cipher stream based on the ~~a~~ second key to re-encrypt the decrypted video;

simultaneously decrypting and re-encrypting the encrypted video using a combination of the first and the second cipher streams;

conveying the re-encrypted video to a display device to be decrypted by the display device using the second key.

13. The medium of Claim 12, wherein the instructions for simultaneously decrypting and re-encrypting the encrypted video comprise instructions which, when executed by the machine, cause the machine to perform further operations comprising exclusive OR-ing the encrypted video with the cipher stream combination.

14. The medium of Claim 12, wherein the cipher stream combination comprises a result of exclusive OR-ing the first and second cipher streams.

15. The medium of Claim 12, wherein the first key and the second key have symmetric agreement.

16. The medium of Claim 12, wherein the instructions for receiving first and second keys comprise instructions which, when executed by the machine, cause the machine to perform further operations comprising receiving one or more of the first key and the second key over a secure authenticated channel.

17. An apparatus comprising:

a content interface to receive encrypted video from a broadcast video source;

a key interface to receive first and second encryption keys from a key server;

a computing device to generate a first cipher stream based on the ~~a~~ first key for decrypting the encrypted video, to generate a second cipher stream based on a second key to re-encrypt the encrypted video and to simultaneously decrypt and re-encrypt the

received encrypted video using a combination of the first and the second cipher streams; and

a sink interface to convey the re-encrypted video to a display device to be decrypted by the display device using the second key.

18. The apparatus of Claim 17, further comprising a secure authenticated channel interface to receive one of either the first key or the second key.

19. The apparatus of Claim 17, wherein the first key and the second key have symmetric agreement and wherein the combination of the first and the second cipher streams is a result of exclusive OR-ing the encrypted video with an encryption stream.

20. The apparatus of Claim 17, wherein the computing device conveys the second key to the display device to enable the display device to decrypt the re-encrypted video.

21. The apparatus of Claim 17, wherein the computing device includes a broadcast entertainment set-top box.

XI. EVIDENCE APPENDIX

None.

XII. RELATED PROCEEDINGS APPENDIX

None.